Dipl. Elektroing.

Hans-Joachim Otto

Von der Industrie- und Handelskammer öffentlich bestellter und vereidigter Sachverständiger für

- Technik und Systeme der Informationsverarbeitung (insbesondere Telekommunikation)
- Verbindungspreisberechnung

Elektronik-Sachverständiger

Nussbaumweg 16

45259 Essen

Tel.: 0201 860 65 20

Fax: 0201 860 65 29

E-Mail: sv@sv2020.de

Web: **www.sv2020.de**

E-Mail – Sicherheit, Echtheit und Spam-Erkennung

- Ein Leitfaden –

Stand 13.1.2022

Hans-Joachim Otto
ö.b. Sachverständiger
Nussbaumweg 16
45259 Essen

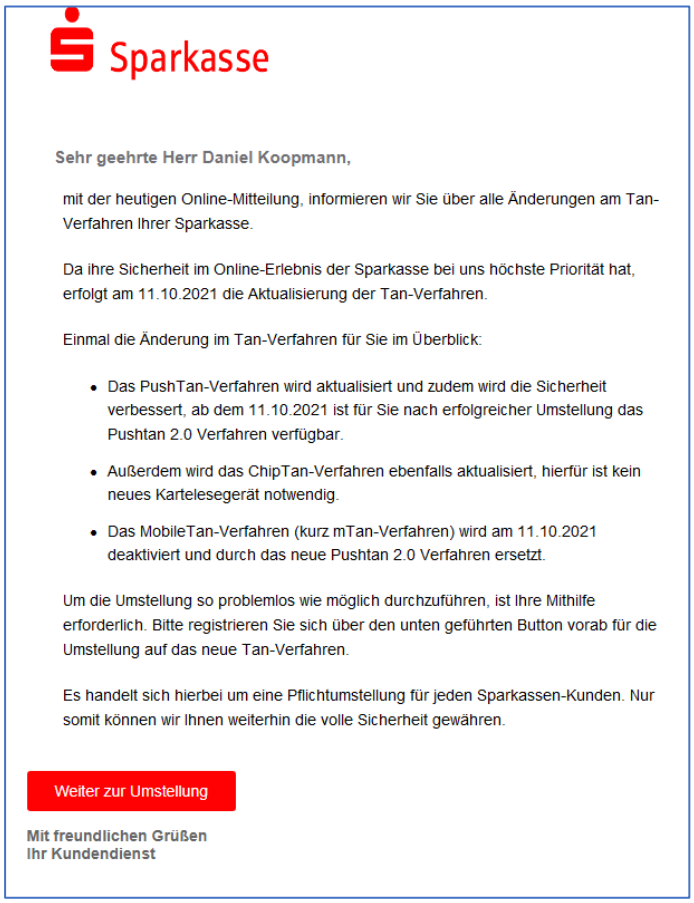
1 Allgemeines

Sie erhalten eine Mail mit eher dubiosem Inhalt und fragen sich, was es damit auf sich hat.

Dieser Artikel soll Hilfestellungen geben, Spam-Mails zu erkennen und richtig zu reagieren.

1.1 Beispiel 1

Ein bekanntes Beispiel eindeutiger Spam-Mails aus dem Herbst 2021 hat folgenden Inhalt:



Sparkasse

Sehr geehrte Herr Daniel Koopmann,

mit der heutigen Online-Mitteilung, informieren wir Sie über alle Änderungen am Tan-Verfahren Ihrer Sparkasse.

Da ihre Sicherheit im Online-Erlebnis der Sparkasse bei uns höchste Priorität hat, erfolgt am 11.10.2021 die Aktualisierung der Tan-Verfahren.

Einmal die Änderung im Tan-Verfahren für Sie im Überblick:

- Das PushTan-Verfahren wird aktualisiert und zudem wird die Sicherheit verbessert, ab dem 11.10.2021 ist für Sie nach erfolgreicher Umstellung das Pushtan 2.0 Verfahren verfügbar.
- Außerdem wird das ChipTan-Verfahren ebenfalls aktualisiert, hierfür ist kein neues Kartelesegerät notwendig.
- Das MobileTan-Verfahren (kurz mTan-Verfahren) wird am 11.10.2021 deaktiviert und durch das neue Pushtan 2.0 Verfahren ersetzt.

Um die Umstellung so problemlos wie möglich durchzuführen, ist Ihre Mithilfe erforderlich. Bitte registrieren Sie sich über den unten geführten Button vorab für die Umstellung auf das neue Tan-Verfahren.

Es handelt sich hierbei um eine Pflichtumstellung für jeden Sparkassen-Kunden. Nur somit können wir Ihnen weiterhin die volle Sicherheit gewähren.

Weiter zur Umstellung

Mit freundlichen Grüßen
Ihr Kundendienst

Auch wenn diese Spam-Thematik hier eindeutig ist, lässt sich an diesem Beispiel das Grundprinzip der Spam-Erkennung gut nachvollziehen.

1. Hinweis:

mein Name ist nicht "Daniel Knoopmann".

2. Hinweis:

schaut man sich den Kopf der Mail an, dann erkennt man eine Mail-Adresse, die nichts mit der Bank zu tun hat.

Úmstellung des Tan-Verfahrens

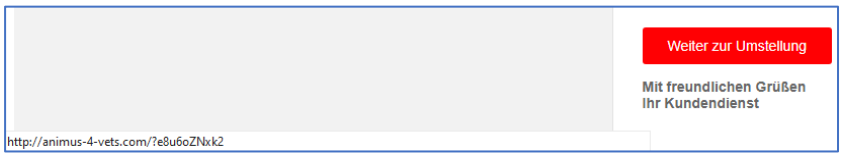
Von "Kundendienst" <h@frontier-ford.com>
An "sv" <sv@sv2020.de>

Dazu ein Sonderzeichen („U“ mit „´“)

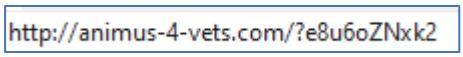
Hans-Joachim Otto
ö.b. Sachverständiger
Nussbaumweg 16
45259 Essen

3. Hinweis:

schiebt man die Maus auf den Link (roter Bereich "Weiter zur Umstellung") ohne darauf zu klicken, dann wird ein Link angezeigt, der sicher nicht zur Bank gehört.



Hier noch mal vergrößert:



Weitere Aufschlüsse gibt der Inhalt der Mail, der normalerweise nicht sichtbar ist.

Dazu klickt man mit der rechten Maus-Taste auf die Mail - bei den üblichen Mail-Programmen wie Outlook, Thunderbird und emClient. Im Untermenü wählt man „Seitenquelltext anzeigen“.

Das ist dann der Inhalt und die wirkliche Struktur einer Mail, wie sie übertragen wird.

Im Quell-Text der Mail sind die verschiedenen Stufen der Übertragung enthalten, jedes System der Übertragungskette vermerkt hier von wem man die Mail erhalten hat und an wen diese weitergeleitet wurde.

Dabei ist die Leseweise von unten nach oben. Vor dem Inhalt (als solcher in der Regel einfach zu erkennen) stehen die Ersteller- und Ausgangs-Transportinformationen:

```
From: "Kundendienst" <h@frontier-ford.com>
Subject: =?utf-8?B?w5ptc3RlbGxlbmcgZGVzIFRhbilWZXJmYWhyZW5z?=
To: "sv" <sv@sv2020.de>
Content-Type: multipart/related; boundary="cg8XYU48UybLsXyLGxHipiQ=_OASppDHQE"
MIME-Version: 1.0
Date: Thu, 7 Oct 2021 00:59:20 +0000
Message-ID: <0102017c584308fe-c05d69e8-3929-4848-af2e-dbldd89bf9c5-000000@eu-west-1.amazonses.com>
Feedback-ID: 1.eu-west-1.kRK8R2wEolKTDOcLa8f2ZiUPz2fViILGopQd4lExc9Y=:AmazonSES
X-SES-Outgoing: 2021.10.07-54.240.4.9
```

Die Angabe „amazonses.com“ verleitet uns zur Google-Suche.

Hans-Joachim Otto
ö.b. Sachverständiger
Nussbaumweg 16
45259 Essen

Es handelt sich also um einer der Amazon-Web-Dienste, mit dem Massen-Mails verschickt werden können.

Damit ist auch klar, dass der Mail-Server meines Providers (smtpin.rzone.de) den Absender als regulären Dienst erkennt, damit werden ja auch „echte“ Werbe-Mails verschickt.

```
Received: from a4-9.smtp-out.eu-west-1.amazonses.com ([54.240.4.9])
    by smtpin.rzone.de (RZmta 47.33.8 OK)
    with ESMTPS id J05459x970xL3hp
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-SHA384 (curve X9_62_prime256v1 with 256 ECDH bits, eq. 3072 bits RSA))
    (Client did not present a certificate)
    for <sv@sv2020.de>;
    Thu, 7 Oct 2021 02:59:21 +0200 (CEST)
```

Man hat sich in diesem Fall also gar nicht die Mühe gemacht, eine individuelle Ansprache des Empfängers der Mails vorzunehmen.

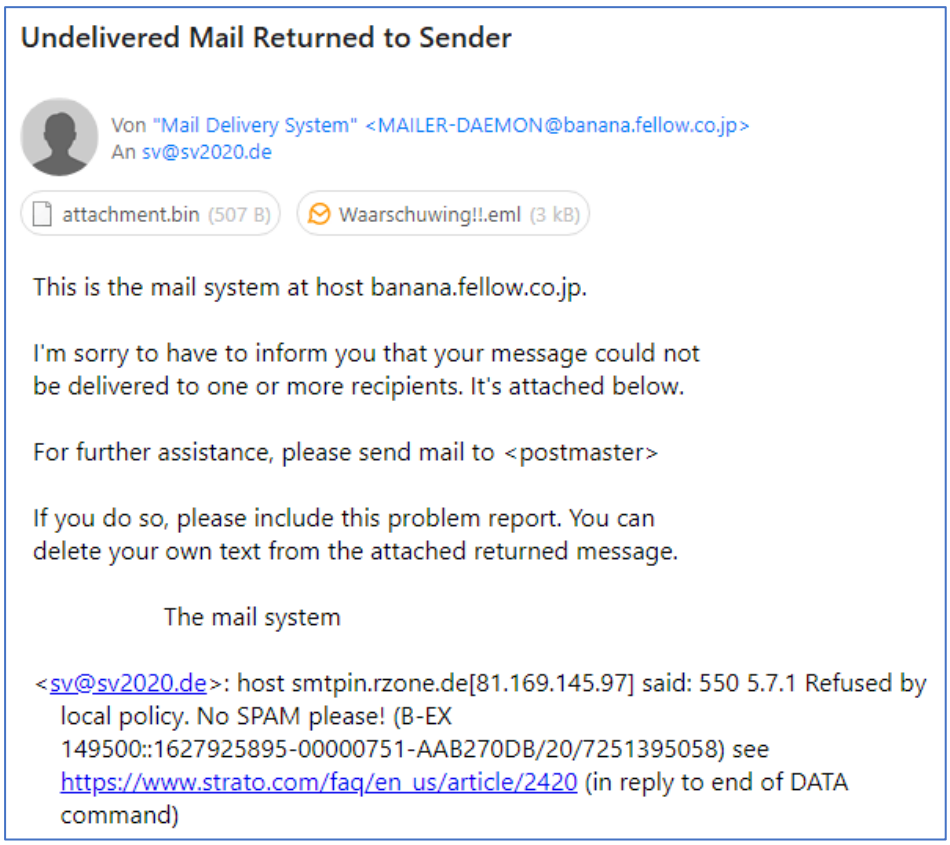
Maßnahme:

Also sofort in den Spam-Ordner verschieben. Es ist wichtig, dass dies über das entsprechende Menü des Mail-Programms erfolgt, damit das Programm sich diese Adresse als Spam merkt (Blacklist).

Würde man die Mail einfach nur löschen, wäre kein Lerneffekt des Mail-Programms verbunden. Außerdem könnte man im Nachhinein nicht nachsehen, ob es bereits ähnliche Spams gab.

1.2 Beispiel 2

Eine schon etwas perfidere Variante ist die Mail, dass der Versand einer Mail gescheitert sei. Man kennt das selbst, wenn man sich bei einer Mail-Adresse vertippt hat. Eine solche Mail kommt dann vom eigenen Mail-Provider.



Undelivered Mail Returned to Sender

Von "Mail Delivery System" <MAILER-DAEMON@banana.fellow.co.jp>
An sv@sv2020.de

attachment.bin (507 B) Waarschuwing!!.eml (3 kB)

This is the mail system at host banana.fellow.co.jp.

I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to <postmaster>

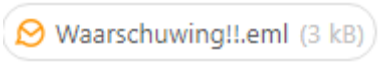
If you do so, please include this problem report. You can delete your own text from the attached returned message.

The mail system

<sv@sv2020.de>: host smtpin.rzone.de[81.169.145.97] said: 550 5.7.1 Refused by local policy. No SPAM please! (B-EX 149500::1627925895-00000751-AAB270DB/20/7251395058) see https://www.strato.com/faq/en_us/article/2420 (in reply to end of DATA command)

Hans-Joachim Otto
ö.b. Sachverständiger
Nussbaumweg 16
45259 Essen

Die Mail wurde von einer Adresse: "MAILER-DAEMON@banana.fellow.co.jp" versendet. Hat also nichts mit meinem Mail-Provider Strato zu tun.

Es soll wohl die eingebettete Mail 

angeklickt werden.

Maßnahme:

Wie zuvor in den Spam-Ordner verschieben.

1.3 Beispiel 3

Ein Freund hat das Problem, dass er regelmäßig und zu gleichen Zeiten eine Mail bekommt, dass ein Mail-Versand gescheitert sei. Ist das nun Spam? Oder hat jemand das Mail-Konto gehackt?

Von: "WEB.DE Mailer Daemon" <keineantwortadresse@web.de>
Datum: 3. Januar 2022
An: [redacted]@web.de
Cc:
Betreff: Mail delivery failed: returning message to sender

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of
its recipients. This is a permanent error.

The following address failed:

[redacted]@web.de:
SMTP error from remote server for RCPT TO command, host: mx-ha03.web.de (212.227.15.17) reason: 550 Requested action not taken: mailbox unavailable

Der Quelltext dieser dubiosen Mail wird auch mitgeschickt und ermöglicht damit schnell eine Diagnose:

```
--- The header of the original message is following. ---

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=web.de;
      s=dbaedf251592; t=1641164462;
      bh=T2zbn4180aN1A1Km06l3wLPY94lWNX2D4ema7fN/PP4=;
      h=X-UI-Sender-Class:From:To:Date:Subject;
      b=Qqw0k9xKf7szPU5bKqfHOs6+Zt3AEBHBjkzDIfNmvJygdxz7Q0gK3vFPE1W6UofTl
       yuz1kafQs0BpvQXn8Wyxjk53iuPwxamzyt54Ax0EqzYuA9zbcDvtGih4U65VHLqxVQ
       ur5gZoPis5tzZYu3y0Af3hOQKNyCywUpI0NOg3Qw=
X-UI-Sender-Class: c548c8c5-30a9-4db5-a2e7-cb6cb037b8f9
Received: from fritzbox ([94.[redacted]]) by smtp.web.de (mrweb106
 [213.165.67.124]) with ESMTPSA (Nemesis) id 1M76XN-1n2mnq3Yyd-008iia for
 <[redacted]@web.de>; Mon, 03 Jan 2022 00:01:01 +0100
Message-Id: <1639695.mmailer3371647853@fritz.box>
From: "=?UTF-8?B?RlJJVFohUmVwZWF0ZXIgMjQwMA==?=" <[redacted]@web.de>
To: <[redacted]@web.de>,
Date: Mon, 3 Jan 2022 00:01:01 +0100
Subject: =?UTF-8?B?RlJJVFohUmVwZWF0ZXItSW5mbzogTnV0enVuZ3MtIHVuZCBWZXJiaW5
Mime-Version: 1.0
Content-Type: text/html;
      charset="utf-8"
```

Der Absender war demnach die eigene FritzBox mit der eigenen IP-Adresse.

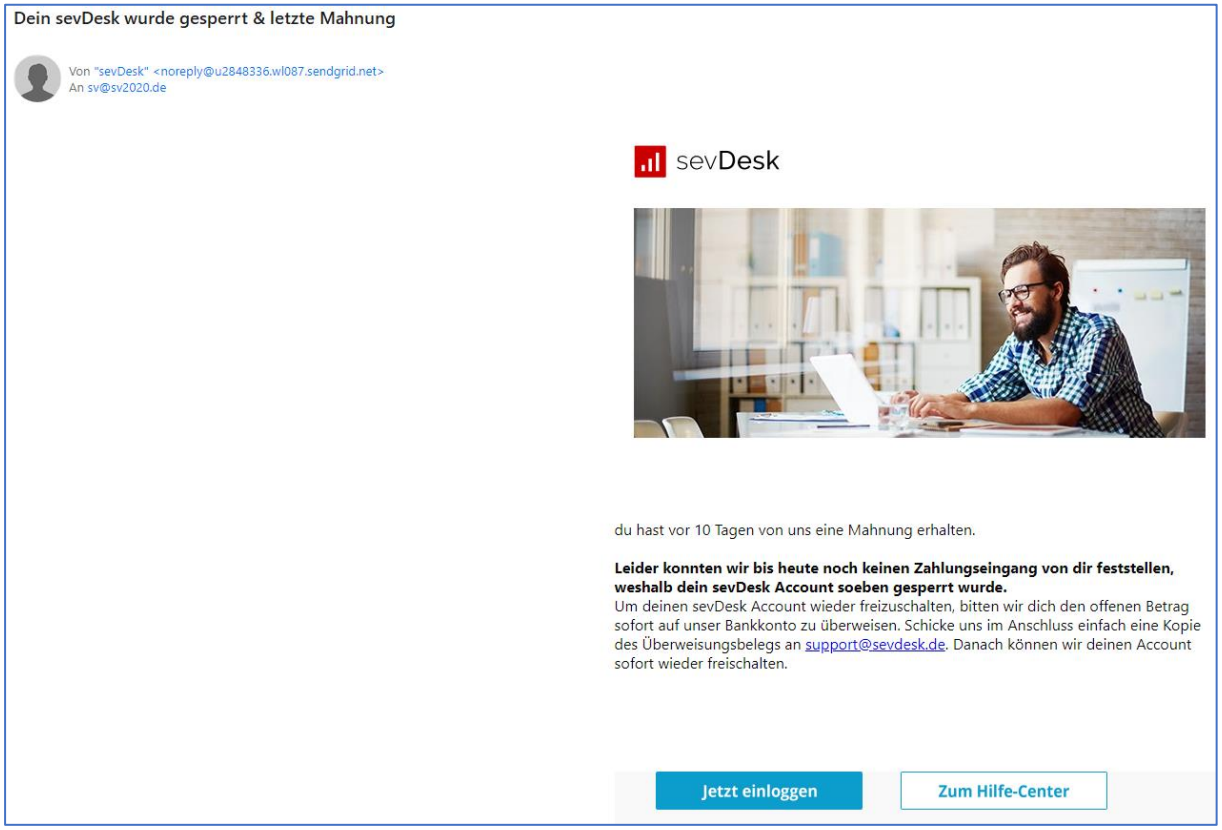
Der Freund hatte im Menü seiner FritzBox unter „System“ – „Push Service“ eingestellt, dass bestimmte Zustände per Mail mitgeteilt werden sollen. Allerdings war die Empfänger-Adresse falsch eingegeben worden.

Der Nachrichten-Quelltext kann also auch in einem solchen Fall sehr hilfreich sein!

Hans-Joachim Otto
ö.b. Sachverständiger
Nussbaumweg 16
45259 Essen

1.4 Beispiel 4

Die Betreff-Zeile der Mail sagt: „Dein sevDesk wurde gesperrt & letzte Mahnung“



Ich habe kein sevDesk-Konto, aber es könnte ja jemand sich für mich ausgegeben haben (Identitätsdiebstahl).

Schaut man sich den Quelltext an, dann wird wieder ein Massen-Mailversender (sendgrid.net, einfach bei Google suchen nach „wer ist sendgrid.net“) erkennbar. Bestsrv hat ähnliche Ambitionen.

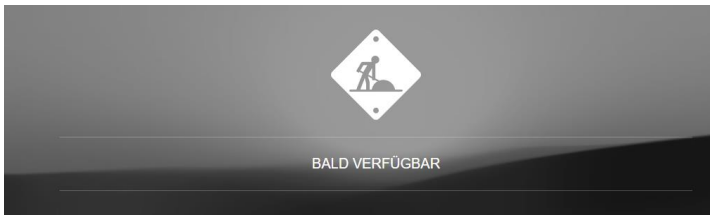
```
Received: from v2202108152487160898.bestsrv.de ([2a03:4000:59:bc1:c8d7:b2ff:fe2d:a638])
    by smtpin.rzone.de (RZmta 47.37.6 OK)
    with ESMTPS id 06709by0DAhjI69
    (using TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256 bits))
    (Client did not present a certificate)
    for <sv@sv2020.de>;
    Thu, 13 Jan 2022 11:43:45 +0100 (CET)
Received: from 127.0.0.1 (localhost [127.0.0.1])
        by v2202108152487160898.bestsrv.de (8.15.2/8.15.2/Debian-10) with SMTP id 20DAhjmv005511
        for <sv@sv2020.de>; Thu, 13 Jan 2022 11:43:45 +0100
Date: Thu, 13 Jan 2022 11:43:45 +0100
Message-Id: <202201131043.20DAhjmv005511@v2202108152487160898.bestsrv.de>
Content-Type: multipart/alternative;
 boundary="===============0516942214978730337=="
MIME-Version: 1.0
Subject: Dein sevDesk wurde gesperrt & letzte Mahnung
From: sevDesk<noreply@u2848336.wl087.sendgrid.net>
To: sv@sv2020.de
```

Spätestens beim Sichten der Link-Adresse bei „jetzt einloggen“ wird klar, dass dort eine Fake-Website aufgebaut worden ist:

https://app.sevdesk-service.de.immobilienbewertung-schumacher.de/info/sev.htm

Hans-Joachim Otto
ö.b. Sachverständiger
Nussbaumweg 16
45259 Essen

Derartige Links liest man immer von rechts nach links. Die Domain ist in Deutschland registriert „.de“. Dann wird es aber mit „immobilienbewertung-schumacher“ äußerst dubios. Diese Website ist „bald verfügbar“.



Der „Login-Link“ verweist auf einen Website-Editor bei 1&1.

Man hat hierzu also Unterseiten (Subdomains) eingerichtet (app.sevdesk-service.de), um hierüber Fake-Seiten erreichbar zu machen.

Es ist also alles ein Betrugsversuch.

2 E-Mail-Signaturen und Verschlüsselung

Wie kann man jetzt erreichen, dass der Empfänger einer Mail auch sicher sein kann, dass der Absender „echt“ ist, ohne im Nachrichten-Quelltext zu forschen?

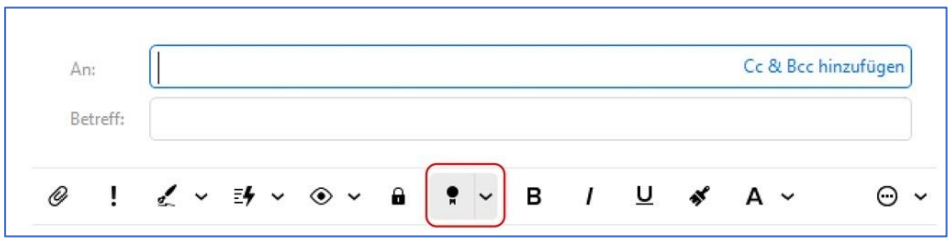
Hierzu gibt es Signaturen.

2.1 Grundlagen und Funktionen

Dazu braucht man erst einmal ein Zertifikat, welches man bei einer Zertifizierungsstelle beantragen kann. Ich nutze ein S/MIME-Zertifikat, da hierbei die Mail-Adresse durch eine zertifizierte Stelle verifiziert wird.

Ich habe meines für die Mail sv@sv2020.de bei Sectigo (früher Comodo) über einen der deutschen Vertriebspartner (19€ pro Jahr in der Basis-Version ohne Signaturkarte) bezogen.

Bei der Erstellung einer neuen Mail zeigt mir dann das Mail-Programm (hier emClient) an, dass standardmäßig signiert wird. Mit dem Schloss-Symbol wird die Verschlüsselung eingeschaltet.



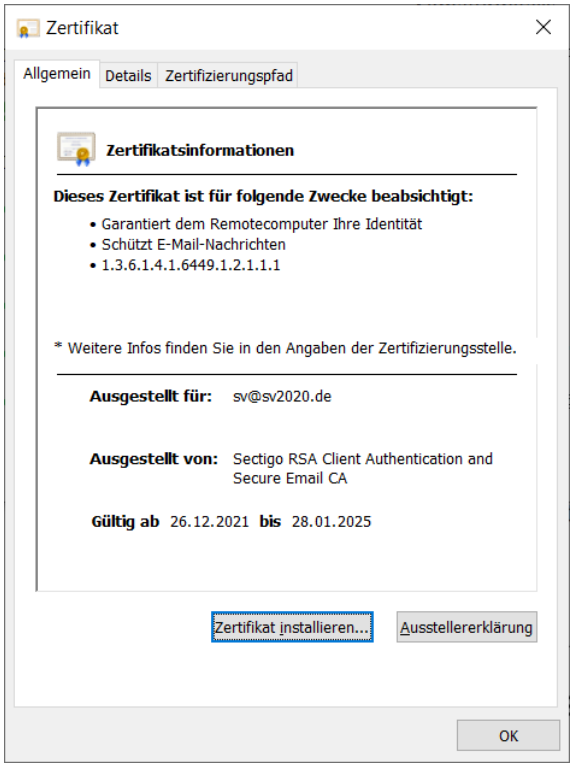
Bei einer versendeten Mail wird angezeigt, dass sie signiert wurde:

Diese Information erscheint auch beim Empfänger.

Dieser kann jetzt den Link „signiert“ anklicken und erhält dann die Informationen zum Inhaber des Zertifikats:

Hans-Joachim Otto
ö.b. Sachverständiger
Nussbaumweg 16
45259 Essen

Unter „Zertifikatsdetails“ gibt es noch weitere Informationen:



Diese Basis-Signatur ist auf jeden Fall sinnvoll. Für die Generierung des Zertifikats ist ein privater Schlüssel notwendig, der im eigenen Rechner erzeugt wird und stets geheim bleiben muss.

Um jetzt die Identität zu fälschen, müsste ein „neues“ Zertifikat generiert werden, das aber fest mit der Mail „sv@sv2020.de“ verknüpft ist. Dazu müsste ein Dritter die Zugangsdaten des betreffenden Postfaches besitzen und dann entsprechend missbrauchen.

2.2 Verschlüsselung

Ein Zertifikat (das entspricht in anderer Bezeichnungsweise einem „öffentlichen Schlüssel“) ermöglicht die Verschlüsselung von Mails.

Der Empfänger kann eine mit dem öffentlichen Schlüssel (Zertifikat) verschlüsselte Mail nur mit seinem privaten (geheimen) Schlüssel entschlüsseln.

Hans-Joachim Otto
ö.b. Sachverständiger
Nussbaumweg 16
45259 Essen

Das ist genauso einfach wie das Signieren. Man merkt gar nicht mehr, dass verschlüsselt wird.

2.3 Software-Erfordernisse

Die üblichen Mail-Programme wie Outlook, Thunderbird und emClient sind die optimale Basis für Signaturen und Verschlüsselung. Die entsprechenden Programm-Module sind standardmäßig vorhanden.

Der private Schlüssel (meist mit Dateiendung „.pfx“) wird im entsprechenden Menü importiert. Dann wird nur noch eingestellt, dass das Zertifikat (*.cer-datei) immer mitgesendet wird.

Bei Android-Endgeräten kann beispielsweise die App „FairEmail“ die gleiche Funktion erfüllen. Die pfx-Datei überträgt man mittels USB-Kabel auf das Endgerät und importiert sie dann in die App.

Bei Apple-Endgeräten ist diese Funktionalität bereits standardmäßig im System und im Mail-Programm enthalten. Die Zertifikate werden in „Einstellungen – Allgemein – VPN und Geräteverwaltung“ angezeigt.

Der Transfer kann z.B. über eine Mail mit entsprechendem Anhang erfolgen, da Apple eher restriktiv die Übertragung von Dateien über eine lokale kabelgebundene Datenverbindung vorsieht.

WIE man einen Schlüssel bzw. ein Zertifikat generiert ist in den Anleitungen bei den verschiedenen Vertriebspartnern ausführlich beschrieben.